IN THE CLAIMS:

Amended claims follow:

1. (Cancelled)

2. (Previously Amended) A method for generating an authentication tag for a message, comprising:

processing a portion of the message using a first function to produce an interim output; and

processing the interim output using a second function to produce the authentication tag;

wherein the message includes a number of message parts, and wherein the portion of the message processed is selected by using a pseudorandom probabilistic function to determine whether each message part is provided as input to said first function.

3. (Original) The method of claim 2, wherein said message parts are 64-bit words.

4. (Cancelled)

5. (Previously Amended) A method for generating an authentication tag for a message, comprising:

processing a portion of the message using a first function to produce an interim output; and

processing the interim output using a second function to produce the authentication tag;

wherein the message includes a number of message parts, and wherein the portion of the message processed is selected by:

defining a message selection percentage p; and

using a pseudorandom probabilistic function, uniform over an interval [1, 2L], where $L = 1/p$ and p is a message selection percentage, to determine offsets between message parts which are provided as input to said first function.

6.- 9. (Cancelled)

10. (Previously Amended) A device for generating an authentication tag for a message, comprising:

a first hashing module that processes a portion of the message to produce an interim output; and

a second hashing module that processes said interim output to produce the authentication tag;

wherein the message includes a number of message parts, and wherein the portion of the message processed is selected by using a pseudorandom probabilistic function to determine whether each message part is provided as input to said first hashing module.

11. (Original) The device of claim 10, wherein said message parts are 64-bit words.

12. (Cancelled)

13. (Previously Amended) A device for generating an authentication tag for a message, comprising:

a first hashing module that processes a portion of the message to produce an interim output; and

a second hashing module that processes said interim output to produce the authentication tag;

wherein the message includes a number of message parts, and wherein the portion of the message processed is selected by:

defining a message selection percentage p; and

using a pseudorandom probabilistic function, uniform over an interval [1, 2L], where $L = 1/p$ and p is a message selection percentage, to determine offsets between message parts which are provided as input to said first hashing module.

14. - 16. (Cancelled)

17. (New) The method of claim 2, wherein the method is carried out utilizing a system including a local security and resource manager.

18. (New) The method of claim 2, wherein the method is carried out utilizing a system including a network application.

19. (New) The method of claim 2, wherein the method is carried out utilizing a system including a security association and key management module.

20. (New) The method of claim 2, wherein the method is carried out utilizing a system including a security services module.

21. (New) The method of claim 20, wherein the security services module includes a partial authentication portion.

22. (New) The method of claim 20, wherein the security services module includes a higher-speed lower-strength portion.

23. (New) The method of claim 20, wherein the security services module includes a lower-speed higher-strength portion.

24. (New) The method of claim 5, wherein the method is carried out utilizing a system including a local security and resource manager.

25. (New) The method of claim 5, wherein the method is carried out utilizing a system including a network application.

26. (New) The method of claim 5, wherein the method is carried out utilizing a system including a security association and key management module.

27. (New) The method of claim 5, wherein the method is carried out utilizing a system including a security services module.

28. (New) The method of claim 27, wherein the security services module includes a partial authentication portion.

29. (New) The method of claim 28, wherein the security services module includes a higher-speed lower-strength portion.

30. (New) The method of claim 29, wherein the security services module includes a lower-speed higher-strength portion.